Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования

"Санкт-Петербургский государственный университет промышленных технологий и дизайна"

ВЫСШАЯ ШКОЛА ТЕХНОЛОГИИ И ЭНЕРГЕТИКИ

УТВЕРЖДАЮ
Директор ВШТЭ
_____ П.В.Луканин
«06» 06 2018 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.09 (индекс дисциплины) Хранение и защита компьютерной информации в АСУ (Наименование дисциплины)

Кафедра 1 (Код) Информационно-измерительных технологий и систем управления (Наименование кафедры)

Направление подготовки: 15.04.04 АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И ПРОИЗВОДСТВ

Профиль подготовки: Системы автоматизации и управления технологическими процессами

Уровень образования: Магистратура

План учебного процесса

Составляющие учебного плана		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	72		72
	Аудиторные занятия	18		8
	Лекции	0		0
	Лабораторные занятия	0		0
	Практические занятия	18		8
	Самостоятельная работа	54		60
	Промежуточная аттестация	0		4
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачёт	3		4
	Контрольная работа			
	Курсовой проект (работа)			4
Общая трудоемкость дисциплины (зачетные единицы)		2		2
Семестр		3		4

Санкт-Петербург
2018

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования

по направлению подготовки 15.04.04 АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И ПРОИЗВОДСТВ

На основании учебных планов № m150404, zm150404

Кафедра-разработчик: Информационно-измерительных технологий и систем управления
(наименование кафедры)

Заведующий кафедрой: Сидельников В.И.
(Ф.И.О. заведующего, подпись)

СОГЛАСОВАНИЕ:

Выпускающая кафедра: Информационно-измерительных технологий и систем управления
(наименование кафедры)

Заведующий кафедрой: Сидельников В.И.
(Ф.И.О. заведующего, подпись)

Методический отдел: Смирнова В.Г.
(Ф.И.О. сотрудника отдела, подпись)

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1:	Базовая		Обязательная		Дополнительно является факультативом
	Вариативная	X	По выбору		

1.2. Цель дисциплины

Сформировать компетенции обучающегося в области основ информационной безопасности, практических умений и навыков применения современных технологий обеспечения защиты информации, и безопасного использования программных средств в автоматизированных системах управления.

1.3. Задачи дисциплины

- Рассмотреть модели и методы представления и хранения информации;
- Рассмотреть существующие угрозы безопасности информации;
- Раскрыть принципы и методы подбора и применения современных методов и способов защиты информации;
- Приобрести практические навыки по защите информации и работы с современными средствами криптографического преобразования информации.

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ОК- 2	готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	2, 3
Планируемые результаты обучения Знать: 1) Основные методы использования современных программных средств для обеспечения информационной безопасности; 2) Механизмы возникновения нарушений информационной безопасности. Уметь: 1) Использовать методы защиты информационных систем; 2) Ориентироваться в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения. Владеть: 1) Терминологией в области защиты информационной безопасности; 2) Навыками работы современными сетевыми фильтрами и средствами криптографического преобразования информации.		
ПК-18	способностью осуществлять управление результатами научно-исследовательской деятельности и коммерциализацией прав на объекты интеллектуальной собственности, осуществлять ее фиксацию и защиту	1
Планируемые результаты обучения Знать: 1) Основы коммерциализации прав на объекты интеллектуальной собственности; 2) Механизмы управления результатами научно-исследовательской деятельности с целью ее хранения и защиты. Уметь: 1) Использовать методы хранения и защиты информации в научно-исследовательской деятельности; 2) Осуществлять защиту результатов научно-исследовательской деятельности. Владеть: 1) Терминологией в области хранения и защиты компьютерной информации; 2) Навыками осуществлять коммерциализацию прав на объекты интеллектуальной собственности,		

Код компетенции	Формулировка компетенции	Этап формирования
соблюдая методы ее защиты.		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

- Философские вопросы теоретических знаний (ОК-2)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Понятия и определения системы баз данных			
Тема 1. Основные понятия баз данных Информация, данные, знания. Типы структур, модели данных. Операции над данными. Ограничения целостности. Администрирование базы данных. Механизмы среды хранения и архитектура БД. Структура хранимых данных. Управление пространством памяти и размещением данных. Виды адресации хранимых записей. Способы размещения данных и доступа к данным в БД.	12		12
Тема 2. Доступ и защита данных в базах данных Угрозы безопасности БД: общие и специфические. Требования безопасности БД. Защита от несанкционированного доступа (НСД). Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Многоуровневая защита.	10		12
Текущий контроль 1. Опрос	2		
Учебный модуль 2. Основы информационной безопасности			
Тема 3. Основные понятия и угрозы информационной безопасности Понятие информационной безопасности. Основные составляющие ИБ. Важность и сложность проблемы ИБ. Наиболее распространенные угрозы ИБ. Наиболее распространенные угрозы доступности, конфиденциальности, целостности. Вредоносное программное обеспечение. Основные правила защиты от «компьютерных вирусов». Обзор и методика использования антивирусных программ. Восстановление пораженных «компьютерными вирусами» объектов.	14		12
Тема 4. Основы законодательства в области информационной безопасности Обзор российского законодательства в области информационной безопасности. Обзор зарубежного законодательства в области информационной безопасности. Текущее состояние российского законодательства в области информационной безопасности. Стандарты и спецификации в области информационной безопасности.	10		12
Тема 5. Программно-технические меры обеспечения компьютерной безопасности информационных систем Основные понятия программно-технического уровня информационной безопасности. Идентификация и аутентификация, управление доступом. Парольная аутентификация. Одноразовые пароли. Применение биометрических систем идентификации. Протоколирование и аудит, шифрование, контроль целостности. Методы криптографического шифрования. Экранирование. Архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности. Обеспечение высокой доступности. Отказоустойчивость и зона риска. Программное обеспечение промежуточного слоя. Обеспечение отказоустойчивости и обслуживаемости.	16		12
Текущий контроль 2. Опрос	2		2
Контрольная работа			6
Промежуточная аттестация по дисциплине – Зачет	**6**		**4**
ВСЕГО:	**72**		**72**

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Не предусмотрено.

3.2. Практические занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1.	Механизмы среды хранения и архитектура БД. Способы размещения данных и доступа к данным в БД.	3	3			4	2
2.	Угрозы безопасности БД и защита от них.	3	3			4	2
3.	Основные составляющие информационной безопасности. Угрозы ИБ. Обзор и методика использования антивирусных программ.	3	4			4	2
4.	Обзор российского и зарубежного законодательства в области информационной безопасности	3	3				
5.	Программно-технические меры обеспечения компьютерной безопасности информационных систем. Идентификация и аутентификация, управление доступом.	3	5			4	2
	ВСЕГО:		**18**				**8**

3.3. Лабораторные занятия

Не предусмотрено.

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено.

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1, 2	Опрос	3	2				
2	Опрос					4	1
1, 2	Контрольная работа					4	1

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	3	28			4	20
Подготовка к практическим занятиям	3	20			4	34
Выполнение домашних заданий					4	6
Подготовка к зачету	3	6			4	4

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
	ВСЕГО:	**54**				**60+4**

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Не предусмотрено.

7.2. Система оценивания успеваемости и достижений обучающихся для промежуточной аттестации

традиционная [X] балльно-рейтинговая [ ]

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Молдованова, О.В. Информационные системы и базы данных [Электронный ресурс]: учебное пособие/ О.В.Молдованова. — Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2014.— 178 c. — (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/45470).

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В.Прохорова. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113c. — (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/43183).

б) дополнительная учебная литература

3. Скрипник, Д.А. Обеспечение безопасности персональных данных [Электронный ресурс]: электрон. текстовые данные/ Д.А.Скрипник. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121c. — (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/16708).

4. Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс]: электрон. текстовые данные/ Д.А.Скрипник. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 c. — (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/16710).

5. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: электрон. текстовые данные/ А.Е.Фаронов. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 c. — (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/16711).

6. Некраха, А.В. Организация конфиденциального делопроизводства и защита информации [Электронный ресурс]: учебное пособие/ А.В.Некраха, Г.А.Шевцова. — М.: Академический Проект, 2015.— 222c. — (ЭБС «IPRbooks»: Режим доступа: http://www.iprbookshop.ru/36849).

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Не предусмотрено.

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. Защита информации. Необходимая информативная база [Электронный ресурс]. URL: http://www.mirash.ru/doki11.html.
2. Защита информации в компьютерных системах [Электронный ресурс]. URL: http://www.hackzona.ru/hz.php?file=article&name=News&sid=40.
3. Разработка системы технической защиты средств обработки хранения и передачи информации [Электронный ресурс]. URL: http://reftrend.ru/462976.html.

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Microsoft Windows 8.1.

2. Microsoft Office Professional 2013.

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Стандартно оборудованная аудитория.
2. Видеопроектор с экраном.

8.6. Иные материалы

Презентация на тему «Размещение и доступ к данным в БД».
Презентация на тему «Кодирование и шифрования информации».

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Практические занятия	На практических занятиях разъясняются теоретические положения курса, обучающиеся работают с конкретными ситуациями, овладевают навыками сбора, анализа и обработки информации для принятия самостоятельных решений, навыками подготовки информационных обзоров и аналитических отчетов по соответствующей тематике; навыками работы в малых группах; развивают организаторские способности по подготовке коллективных проектов. Подготовка к практическим занятиям предполагает следующие виды работ: – подготовка ответов к контрольным вопросам; – работа с текстами из списка рекомендуемой основной и дополнительной литературы.
Самостоятельная работа	Самостоятельная работа студента предполагает расширение и закрепление знаний, умений и навыков, усвоенных на аудиторных занятиях путем самостоятельной проработки учебно-методических материалов по дисциплине и другим источникам информации , а также подготовки к зачету. Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством (при участии) преподавателя. Следует предварительно изучить методические указания по выполнению самостоятельной работы. При подготовке к опросам необходимо проработать теоретический материал, рекомендуемую литературу. При подготовке к зачету необходимо ознакомиться с перечнем вопросов, проработать конспекты практических занятий, рекомендуемую литературу, получить консультацию у преподавателя.

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции (этап освоения)	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ОК-2 (2,3)	1. Имеет представление о механизмах возникновения нарушений информационной безопасности и защиты от них 2. Использует современные методы защиты информационных систем для обеспечения информационной безопасности 3. Демонстрирует навыки пользования современными программными средствами для обеспечения защиты информации	1. Устное собеседование 2. Тестовое задание 3. Реферат	1. Перечень вопросов к зачету (40 вопросов) 2. Тестовые задания по вариантам (3 варианта по 40 заданий в каждом) 3. Перечень тем рефератов (30 тем)

Код компетенции (этап освоения)	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ПК-18 (1)	1. Обладает навыками поиска, хранения и обработки информации из различных источников и баз данных 2. Демонстрирует навыки владения терминологией в области хранения и защиты компьютерной информации 3. Способен защитить объекты интеллектуальной собственности, соблюдая методы ее защиты.	1. Устное собеседование 2. Тестовое задание 3. Реферат	1. Перечень вопросов к зачету (40 вопросов) 2. Тестовые задания по вариантам (3 варианта по 40 заданий в каждом) 3. Перечень тем рефератов (30 тем)

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
Зачтено	Обучающийся своевременно выполнил тестовое задание, представил реферат с полностью раскрытой темой, продемонстрировав собственные заключения, выводы и рекомендации по теме. Свободно ориентируется в основных понятиях и терминах по поиску, хранению и защите компьютерной информации; усвоил основную и знаком с дополнительной литературой по обеспечению информационной безопасности, возможно допускает несущественные ошибки в ответе на вопросы преподавателя
Не зачтено	Обучающийся не выполнил тестовое задание, не представил реферат, неспособен сформулировать хотя бы отдельные концепции по хранению и защите компьютерной информации. Попытка списывания, использования неразрешенных технических устройств или пользование подсказкой другого человека.

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов к зачету, разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Обоснуйте, чем отличается база данных от простой совокупности данных	1
2	Назовите основные компоненты системы управления базами данных (СУБД)	1
3	Назовите области применения баз данных и их характеристики	1
4	Сформулируйте по каким признакам и как классифицируют базы данных	1
5	Расскажите об основных функциях СУБД	1
6	Анализ архитектур систем управления базами данных, их достоинства и недостатки	1
7	Способы размещения данных и доступа к данным в БД	1
8	Администрирование базы данных. Основные задачи и пути решения	1
9	Угрозы безопасности баз данных и их характеристики	2
10	Основные требования безопасности баз данных	2
11	Защита от несанкционированного доступа к данным БД	2
12	Проблемы и их решение в обеспечении целостности и правильности данных в БД	2
13	Задачи и средства администратора безопасности баз данных	2
14	Понятие многоуровневой защиты компьютерной информации	2
15	Основные характеристики, определяющие БД как технологию хранения данных и доступа к ним	2
16	Обеспечение безопасности и секретности данных в БД	2

№ п/п	Формулировка вопросов	№ темы
17	Сформулируйте понятия и основные составляющие информационной безопасности	3
18	Обоснуйте важность проблемы компьютерной информационной безопасности	3
19	Наиболее распространенные угрозы, пути и каналы утечки информации	3
20	Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов	3
21	Назовите основные правила защиты от компьютерных вирусов	3
22	Сформулируйте достоинства и недостатки современных антивирусных программ	3
23	Сформулируйте виды противников или «нарушителей» информационной безопасности	3
24	Виды возможных нарушений информационной системы в АСУ	3
25	Сформулируйте понятие законодательного уровня информационной безопасности	4
26	Обоснуйте важность законодательного уровня информационной безопасности	4
27	Критерии безопасности компьютерных систем	4
28	Основные понятия в области лицензирования и сертификации	4
29	Сформулируйте текущее состояние российского законодательства в области информационной безопасности	4
30	В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?	4
31	Объясните порядок оформления и получения лицензий в области информационной безопасности	4
32	Обоснуйте причины отказа в получении лицензии	4
33	Назовитие методы защиты информации	5
34	Сформулируйте понятие «Идентификация пользователей». Классификация методов идентификации пользователей	5
35	Сформулируйте понятия и дайте характеристику «аутентификация пользователей», «парольная аутентификация»	5
36	Дайте определение понятиям «Управление доступом, ограничение, разграничение, разделение доступа к информации» и сформулируйте их основные характеристики	5
37	Сформулируйте преимущества и недостатки метода криптографического преобразования информации	5
38	Экранирование. Классификация межсетевых экранов	5
39	Основные технологии построения защищенных информационных систем	5
40	Обеспечение информационной безопасности в АСУ	5

10.2.2. Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка задания	Ответ
1	Кто является пользователем системой баз данных: а) прикладные программисты б) прикладные программисты, рядовые пользователи, администраторы баз данных в) только администраторы баз данных	б
2	Кто является создателем реляционной модели базы данных: а) Д. Дейт б) Э. Кодд в) А. Бойс	б
3	Основным элементом для хранения информации в реляционных базах данных, является а) поле б) несколько форм в) одна или несколько связанных таблиц	в
4	Многопользовательская система – это: а) система, состоящая из нескольких баз данных б) система, в которой в каждый момент времени к БД могут получить доступ несколько пользователей в) система таблиц	б
5	Сколько баз данных может быть открыто одновременно? а) 1 б) 2 в) неограниченное количество	а

№ п/п	Формулировка задания	Ответ
6	Благодаря работам Эдгара Кодда были созданы базы данных: а) сетевые б) реляционные в) объектно-ориентированные	б
7	Классификация баз данных по характеру информации: а) фактографические базы данных, документальные базы данных б) распределенные базы данных, документальные базы данных, в) базы данных с локальным доступом, документальные базы данных	а
8	Система управления базами данных Microsoft Access является: а) серверной СУБД б) распределенной СУБД в) настольной СУБД	в
9	Виды защиты баз данных: а) учётная запись группы администратора б) приложение, которое используется для управления базой данных в) защита паролем, защита пользователем	в
10	Что не является функцией базы данных: а) обеспечивает хранение информации б) является источником при создании информационных услуг в) заменяет операционную систему	в
11	Поиск данных в базе – это: а) процедура выделения из множества записей подмножества, записи которого удовлетворяют заранее поставленному условию б) определение значений данных в текущей записи в) процедура определения дескрипторов базы данных	а
12	Накопитель данных представляет собой: а) запоминающее устройство б) жесткий диск в) абстрактное устройство для хранения информации	в
13	Операция выделения подмножества значений составной единицы измерения, которые удовлетворяют заранее поставленным условиям: а) переименование б) выборка в) корректировка	б
14	Что можно отнести к техническим мерам информационной безопасности? а) разработку правил, норм, устанавливающих ответственность за компьютерные преступления б) охрану вычислительного центра, тщательный подбор, обучение персонала, ответственного за информационную безопасность в) защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое	в
15	Реляционные базы данных получили своё название благодаря тому, что: а) в них быстро обрабатывается информация б) данные в них представлены в виде таблиц в) в них можно хранить данные сложной структуры	б
16	С какой целью используется процедура сортировки данных? а) для получения итогов различных уровней б) для ввода данных в) для контроля данных	а
17	Что самое главное должно продумать руководство при классификации данных? а) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным б) необходимый уровень доступности, целостности и конфиденциальности в) управление доступом, которое должно защищать данные	б
18	Защита информации это: а) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё б) процесс сбора, накопления, обработки, хранения информации	а

№ п/п	Формулировка задания	Ответ
	в) преобразование информации, распределение и поиск информации	
19	К открытым источникам информации относятся: а) информация, украденная у спецслужб б) газеты, радио, новости в) информация из вскрытого сейфа	б
20	Естественные угрозы безопасности информации вызваны: а) ошибками человека б) корыстными устремлениями злоумышленников в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека	в
21	Искусственные угрозы безопасности информации вызваны: а) деятельностью человека б) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека в) корыстными устремлениями злоумышленников	а
22	Для защиты от злоумышленников необходимо использовать: а) системное программное обеспечение б) прикладное программное обеспечение в) антивирусные программы	в
23	Антивирус, который не только находит зараженные вирусами файлы, но и «лечит» их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние: а) доктор б) сканер в) детектор	а
24	Потенциальные угрозы, против которых направлены технические меры защиты информации: а) потери информации из-за не достаточной установки сигнализации в помещении б) потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей в) потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения	б
25	Что является правовой формой защиты информации? а) разработка специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации; б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации; в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения	а
26	Отношения, связанные с обработкой персональных данных, регулируются законом: а) «Об информации, информационных технологиях» б) Федеральным законом «О конфиденциальной информации» в) Федеральным законом «О персональных данных»	в
27	Как называется умышленно искаженная информация? а) противозаконная б) открытая в) дезинформация	в
28	Государственная тайна это: а) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны б) защищаемые банками и иными кредитными организациями сведения о банковских операциях в) ограничения доступа в отдельные отрасли экономики или на конкретные производства	а
29	Профессиональная тайна это: а) ограничения доступа в отдельные отрасли экономики или на конкретные производства	б

№ п/п	Формулировка задания	Ответ
	б) защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей в) защищаемые банками и иными кредитными организациями сведения о банковских операциях	
30	Что можно отнести к организационным мерам информационной безопасности? а) охрану работоспособности отдельных звеньев информационной системы б) охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д. в) защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем	б
31	Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий? а) нотариальная тайна б) общедоступные сведения в) нотариальный секрет	а
32	Что относят к правовым мерам: а) средства идентификации и аутентификации пользователей б) охрану вычислительного центра и аппаратуры связи в) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур	в
33	Что является наиболее надежным средством предотвращения потерь компьютерной информации при кратковременном отключении электроэнергии? а) установка источников бесперебойного питания б) такого средства не существует в) перекидывать информацию на носитель, который не зависит от энергии	а
34	Программные средства защиты можно разделить на: а) правовые, аппаратные, программные б) административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и т.д. в) криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и т.д.	в
35	Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде? а) оптические б) акустические и виброакустические в) электрические	б
36	Потенциальные угрозы, против которых направлены технические меры защиты информации – это: а) потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей б) потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения в) потери информации из-за не достаточной установки сигнализации в помещении	а
37	Программные средства защиты информации: а) источники бесперебойного питания б) технические средства защиты информации в) средства архивации данных, антивирусные программы	в
38	К каким методам защиты информации относится шумоподавление информационного сигнала? а) полуактивным б) активным в) пассивным	б
39	К средствам охранной сигнализации относятся: а) датчики движения, концевые выключатели б) ограждение, замки, турникеты в) видеокамеры, датчики огня	а

№ п/п	Формулировка задания	Ответ
40	Какие потери информации бывают из-за некорректной работы программ? а) перебои электропитания б) потеря или изменение данных при ошибках программного обеспечения в) ознакомление с конфиденциальной информацией	б

Перечень тем рефератов, разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировки тем рефератов	№ темы
1	Аналитическое обоснование необходимости создания системы технической защиты информации на объекте информатизации	1
2	Актуальные проблемы и пути их решения в области хранения и защиты компьютерной информации в АСУ	1
3	Меры противодействия информационной безопасности в автоматизированных системах обработки данных	1
4	Актуальные задачи и пути их решения по управлению пространством памяти и размещением данных	1
5	Анализ основных операций над данными и механизмы ограничения целостности	1
6	Сравнительный анализ методов воздействия и противодействия в сети Internet	1
7	Актуальность требований и показателей защищенности автоматизированных средств обработки информации	1
8	Понятие атрибутов доступа к файлам. Обзор защиты сетевого файлового ресурса на примерах организации доступа в различных операционных системах	2
9	Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Анализ надежности систем ограничения доступа	2
10	Способы фиксации и анализ фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам	2
11	«Типовые» каналы утечки информации объектов информатизации. Обзор условий и факторов, способствующих утечке информации ограниченного доступа.	2
12	Обзор и анализ мероприятий по обеспечению безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации	2
13	Назначение и краткий анализ общих моделей процесса защиты информации	2
14	Анализ угроз безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности	2
15	Основные направления по защите от враждебных воздействий на компьютерную безопасность. Обоснование необходимых и достаточных условий предотвращения разрушающего воздействия вируса	3
16	Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий	3
17	Важность, сложность и пути решения проблемы информационной безопасности в АСУ	3
18	Обзор мероприятий по защите компьютерной информации в АСУ от потерь	3
19	Анализ мероприятий по защите компьютерной информации в АСУ от вредоносных программ	3
20	Обзор мероприятий по защите компьютерной информации в АСУ от несанкционированного доступа	3
21	Понятие и цели проведения специальных проверок объектов информатизации; обзор и анализ основных этапов проведения проверки	3
22	Необходимость, назначение, общее содержание и анализ организационно- правового обеспечения информационной безопасности	4
23	Анализ основных составляющих национальных интересов в информационной сфере; виды и источники угроз информационной безопасности Российской Федерации	4
24	Принципы государственной политики обеспечения информационной безопасности Российской Федерации. Обзор и анализ.	4
25	Анализ организационно-правовой основы защиты информации в ФСИН России	4
26	Основные направления инженерно-технической защиты компьютерной информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки	5
27	Сравнительный анализ распространённых способов блокирования каналов утечки	5

№ п/п	Формулировки тем рефератов	№ темы
	информации и видов специальных технических средств защиты	
28	Обзор и анализ методов и специальных технических средства, используемых в ходе поисковой операции в целях обеспечения защиты информации	5
29	Сравнительный анализ аппаратных и программно-аппаратных средств криптозащиты данных	5
30	Постановка и решение задач обеспечения информационной безопасности в каналах связи АСУ	5

10.3. Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче зачета и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная	X	письменная		компьютерное тестирование		иная	

10.3.3. Особенности проведения зачета

- Возможность пользоваться записями материалов практических занятий.
- Реферат обучающиеся выполняют самостоятельно в рамках подготовки к зачету (темы рефератов сообщаются преподавателем заранее), непосредственно на зачет обучающиеся приходят с готовыми рефератами.
- Время на выполнение тестового задания – 15 минут.
- Время на подготовку к устному собеседованию – 20 минут, на ответ – 10 минут.